公告本

379308

申請日期	87 年 4 月 15 日
案號	87105738
類別	G09C 1/00

A4
C4

379308

（以上各欄由本局填註）

發明 新型 專利說明書

一、發明新型名稱	中文	密碼化裝置及方法、解碼裝置及方法、以及資訊處理裝置及方法
	英文	
二、發明創作人	姓名	(1) 石黑隆二 (2) 大澤義知 (3) 刑部義雄
	國籍	(1) 日本　(2) 日本　(3) 日本
	住、居所	(1) 日本國東京都品川區北品川六丁目七番三五號 ソニー株式会社
		(2) 日本國東京都品川區北品川六丁目七番三五號 ソニー株式会社
		(3) 日本國東京都品川區北品川六丁目七番三五號 ソニー株式会社
三、申請人	姓名（名稱）	(1) 蘇妮股份有限公司 ソニー株式会社
	國籍	(1) 日本
	住、居所（事務所）	(1) 日本國東京都品川區北品川六丁目七番三五號
	代表人姓名	(1) 出井伸之

經濟部中央標準局員工消費合作社印製

裝　訂　線

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

申請日期	87 年 4 月 15 日
案號	87105738
類別	

A4
C4

（以上各欄由本局填註）

發明 新型 專利說明書

一、發明新型名稱	中文	
	英文	
二、發明創作人	姓名	(1) 佐藤真 (2) 嶋久登 (3) 淺野智之
	國籍	(1) 日本 (2) 日本 (3) 日本
	住、居所	(1) 日本國東京都品川區北品川六丁目七番三五號 ソニー株式会社 (2) 美國加州帕索佛拉斯賽拉托格、美國研究實驗室 US Reserch Laboratories 12610 Paseo Flores Saratoga, CA 95070 U.S.A (3) 日本國東京都品川區北品川六丁目七番三五號 ソニー株式会社
三、申請人	姓名（名稱）	
	國籍	
	住、居所（事務所）	
	代表人姓名	

裝 訂 線

（由本局填寫）

承辦人代碼：	A6 B6
大　　類：	
ＩＰＣ分類：	

本案已向：

國（地區）　申請專利，申請日期：　　案號：　　，□有　□無主張優先權

日本　　1997 年　4 月 23 日　9-106136　　☑有主張優先權

（請先閱讀背面之注意事項再填寫本頁各欄）

有關微生物已寄存於：　　，寄存日期：　　，寄存號碼：

裝　訂　線

A5
B5

四、中文發明摘要（發明之名稱：密碼化裝置及方法、解碼裝置及方法）、以及資訊處理裝置及方法

本發明的課題係爲確實地防止不當的複製。

其解決手段：封以ＤＶＤ播放機１的１３９４介面２６所被暗碼化之資料，介由１３９４匯流排，傳輸到個人電腦２及磁光碟裝置３。在於變更功能未開放給使用者之磁光碟裝置３，以１３９４介面３６的解碼所收訊的資料。對於此點，在於變更功能已開放給使用者之個人電腦２，以１３９４介面４９，用時變鍵ｉ解碼暗碼化的資料，在應用部６１用時段鍵Ｓ進而解碼其解碼其解碼結果。

英文發明摘要（發明之名稱：　　）

（請先閱讀背面之注意事項再填寫本頁各欄）

裝 訂 線

五、發明說明（1）

〔發明所屬領域〕

本發明係爲關於密碼化裝置及方法，解碼裝置及方法，以及資訊處理裝置及方法；特別是關於使其更提高安全性之密碼化裝置及方法，解碼裝置及方法，及其資訊處理裝置及方法。

〔發明背景〕

將代表性電腦等之複數個電子機器，以匯流排相互連接，構成網路，而使其在網路內可以相互收授各種資料。

其結果，例如，以被連接在網路之ＤＶＤ播放器，而可以將從ＤＶＤ所再生的影像資料，介由匯流排，傳輸，顯示在電視顯視機，監視器等的顯示裝置。通常，將ＤＶＤ所再生的影像顯示在顯示裝置而作視聽，係爲在於購入ＤＶＤ的時刻，著作權者所容許的情況。

不過，將ＤＶＤ所再生的資料，複製在其他記錄媒體後使用，一般是不被著作權者所容許。因此，爲了防止介由匯流排（網路）而送出之資料被不法複製，所以在於送出側，使資料密碼化；在於收訊側，解碼此資料已被考慮到。

不過，ＤＶＤ播放器，電視顯像機等的消費性機器（ＣＥ機器），通常是爲了所定的目的而被設計，製造；使使用者無法改造此狀況或組裝其他零件而取得裝置內部的資料且竄改（變更功能）下被製造。對於此點，例如個人電腦，大多數的情況，公開結構體系或電路；由於追加連

五、發明說明（２）

接埠，安裝各種的應用軟體，因而使其可以追加，變更種種的功能。

因此，在於個人電腦，將該內部匯流排上的資料，附加所定的硬體，作成軟體程式，可以較容易地直接查看，改繕個人電腦內部的匯流排上資料。此情況，例如以個人電腦取得在從ＤＶＤ播放器密碼化而傳送至電視顯像機的資料，將此資料解碼後複製，係爲意味著在作成應用軟體下，能容易進件。

換言之，個人電腦，希望是介由匯流排連接進行通訊的連結部，及準備收發訊的資料，利用所收訊的資料之應用部；物理上，邏輯上，在該處使用者可以使用之部分較多。對於此點，在於ＣＥ機器，兩者的連接爲密接，幾乎沒有使用者可以介入的部分。

〔發明所欲解決之課題〕

本發明係爲鑑於此狀況，使其更確實地防止資料的不法複製。

〔實施[illegible]態〕

第[illegible]圖係爲表示適用本發明之資訊處理系統之構成例。在於[illegible]構成例，介由ＩＥＥＥ　１３９４系列匯流排１１而相互連接ＤＶＤ播放器１，個人電腦２，光磁碟裝置３，資料播放收訊裝置４，監視器５，電視顯像機６。

第２圖係及表示其中的ＤＶＤ播放器１，個人電腦２

（請先閱讀背面之注意事項再填寫本頁）

裝　訂

五、發明說明（3 ）

，及磁光碟裝置之內部的更詳細構成例。ＤＶＤ播放器１係爲介由１３９４介面２６而被連接至１３９４匯流排１１。ＣＰＵ２１係爲根據被記憶在ＲＯＭ２２的程式而執行各種的處理；ＲＡＭ係爲在於ＣＰＵ２１執行各種的處理時適切記憶必要的資料或程式。操作部２４，係爲以按鍵，開關，遙控器等所構成，當使用者進行操作時，輸出對應於該操作的訊號。驅動器２５，係爲驅動ＤＶＤ（光碟）（未圖示），使其再生被記錄在該處之資料。ＥＥＰＲＯＭ２７係爲在裝置的電源ＯＦＦ後也能記憶所必要記憶的資訊（此實施形態的情況，鍵資訊）。內部匯流排２８係爲相互連接這些各部分。

磁光碟裝置３具有ＣＰＵ３１至內部匯流排３８。具有與在上述過ＤＶＤ播放器１之ＣＰＵ２１至內部匯流排２８同樣的功能，其說明則省略。不過，驅動器３５，係爲驅動磁光碟（未圖示），在該光磁碟使其記錄或是再生資料。

個人電腦２係爲介由１３９４介面４９而被連接至１３９４匯流排１１。ＣＰＵ４１係爲根據被記憶在ＲＯＭ４２的程式而執行各種的處理。在ＲＡＭ４３，適切記憶著在於ＣＰＵ４１執行各種的處理所必要的資料或程式等。在輸入出介面４４，被連接有鍵盤４５及滑鼠４６等。使其從這些裝置所輸入的訊號輸出至ＣＰＵ４１。另外，在輸入出介面４４，被連接有硬碟（ＨＤＤ）４７，使其可以在該處記錄再生資料，程式等。在輸入出

（請先閱讀背面之注意事項再填寫本頁）

訂

五、發明說明（４）

介面４４另外使其適切裝著擴充埠４８，可以附加必要的功能。在ＥＥＰＲＯＭ５０使其記憶在電源ＯＦＦ後也能保持所必要的資訊（此實施形態的情況，各種的鍵入資訊）。例如，以ＰＣＩ（Peripheral Component Interconnect），區間匯流域所構成之內部匯流排５１，係爲使其相互連接這些各部分。

然而，此內部匯流排５１係爲對使用者開放；使用者係爲在擴充埠４８適切連接所定的連接埠，作成所定的軟體程式後安裝，而使其適切收訊以內部匯流排５１所被傳輸的資料。對於此點，在於ＤＶＤ播放器１或磁光碟裝置３等的消費性電子（ＣＥ）裝置，內部匯流排２８或內部匯流排３８，來被開放給使者，只限於進行特殊的改造等，使其無法取得傳輸到該匯流排之資料。

其次，說明在所定的始源端與接收端之間所進行之鍵認處理。此鍵認的處理，係爲如第３圖所示，在於作爲始源端的例如作爲預先被記憶在ＤＶＤ播放器１的ＲＯＭ２２之軟體程式的１種之固件２０，與作爲接收端的例如被記憶在個人電腦２的ＲＯＭ４２，作爲ＣＰＵ４１所處理的軟體程式的１種之許可管理６２之間被進行。

第４圖係爲表示在於始源端（ＤＶＤ播放器１）與接收端（個人電腦２）之間所進行的鍵認順序。在ＤＶＤ播放器１的ＥＥＰＲＯＭ２７，預先被記憶有服務鍵（service_key）及函數（hash）。這些都是從著作權者，所

（請先閱讀背面之注意事項再填寫本頁）

五、發明說明（５）

提供給此ＤＶＤ播放器１的使用者；各使用者將此秘密的保管在ＥＥＰＲＯＭ２７。

服務鍵係爲被加諸在著作權者所提供的每個資訊；在於以此１３９４匯流排１１所構成之系統爲共通的。然而，在於本說明書，系統係爲表示以複數個裝置所構成之全體裝置。

ｈａｓｈ函數係爲對於任意長的輸入，輸出６４位元或是１２８位元的固定長資料；設爲Ｙ（＝ｈａｓｈ（ｘ））時，造成求出ｘ會有困難，且求出成爲ｈａｓｈ（ｘ１）＝ｈａｓｈ（ｘ２）之ｘ１及ｘ２的組合也會有困難之函數。作爲１方向ｈａｓｈ關數的代表性函數，已知有ＭＤ５或ＳＨＡ。關於此１方向Ｈａｓｈ函數，在 Bruce Schneier著的「Applied Cryptography (Second Edition), Wiley」已被詳細地解說。

另則，作爲接收端之例如個人電腦２，係爲將從著作權等所供予個人所屬之固有識別編號（ＩＤ）及許可鍵（license_key）祕密的保持在ＥＥＰＲＯＭ５０。此許可鍵係爲對於連結幾位元的ＩＤ及ｎ位元的服務鍵所得到的ｎ＋ｍ位元之資料（ID｜｜serviec_key），適用ｈａｓｈ函數而得到之值。即是許可鍵以下式表示。

license_key=hash(ID｜｜serviec_key)

作爲ＩＤ例如可以使用１３９４匯流排１１的規格所

五、發明說明（６）

訂定之 node_unique_ID。此 node_unique_ID，係爲如第５圖所示，以８位元組（６４位元）所構成；最初的３位元組，係爲以ＩＥＥＥ所管理，從ＩＥＥＥ提供給電子機器的各製造廠。另外，下位５位元組，係爲各製造廠可以提供給使用者所使用的裝置。各製造廠，例如對於下位５位元組，在系列使其１台分配１個編號，使用了全部５位元組分時，上位３位元組進行接受提供形成爲別的編號之 node_unique_ID，然而，針對該下位５位元組，使其１台分配１個編號。因此，此 node_unique_ID，不拘限於製造廠，每一台都是不同，在各裝置形成爲固有的ＩＤ。

在於步驟Ｓ１，ＤＶＤ播放器１的固件２０，係爲控制１３９４介面２６，介由１３９４匯流排１１而對於個人電腦２要求ＩＤ。個人電腦２的許可管理６２，係爲在於步驟Ｓ２，收訊此ＩＤ的要求。即是１３９４介面４９，係爲介由１３９４匯流排１１而收訊從ＤＶＤ播放器７所傳輸到來的ＩＤ要求訊號，則將此訊號輸出至ＣＰＵ４１。ＣＰＵ４１的許可管理６２，係爲接受此ＩＤ要求時，在於步驟Ｓ３，讀出被記憶在ＥＥＰＲＯＭ５０的ＩＤ，將此ＩＤ介由１３９４介面４９而從１３９４匯流排１１傳輸至ＤＶＤ播放器。

在於ＤＶＤ播放器，在步驟Ｓ４，１３９４介面２６接收此ＩＤ，則此ＩＤ被供給到以ＣＰＵ２１所動作的固件２０。

固件２０係爲在於步驟Ｓ５，結合從個人電腦２受理

（請先閱讀背面之注意事項再填寫本頁）

訂

線

五、發明說明（7）

傳輸之ＩＤ，及被記憶在ＥＥＰＲＯＭ２７之服務鍵，而生成資料（ＩＤ｜｜serviec_key），對於此資料，如次式所示適用Ｈａｓｈ函數，生成鍵ｌＫ。

lk=hash(ID | | serviec_key)

其次，在於步驟Ｓ６，固件２０係爲生成密碼鍵ｓｋ。此密碼鍵ｓｋ之詳情於後述，但此密碼鍵ｓｋ係爲在於ＤＶＤ播放器１及個人電腦２分別被利用，作爲時段鍵。

其次，在於步驟Ｓ７，係爲以步驟Ｓ５所生成之鍵ｌｋ作爲鍵，將步驟Ｓ６所生成之密碼鍵ｓｋ密碼化，而得到密碼化資料（密碼化鍵）ｅ。即是運算下式。

e=Enc (lk,sk)

然而，Ｅｎｃ（Ａ，Ｂ）係爲意味著以共通鍵密碼方式，用鍵Ａ，而將資料Ｂ密碼化。

其次，在步驟Ｓ８，固件２０係爲將步驟Ｓ７所生成之密碼化資料ｅ傳輸到個人電腦２。即是此密碼化資料ｅ，從ＤＶＤ播放器１的１３９４介面２６，介由１３９４匯流排１１而被傳輸到個人電腦２。在於個人電腦２，在步驟Ｓ９，介由１３９４介面４９而收訊此密碼化資料ｅ。許可管理６２，係爲將經該過程所收訊的密碼化資料記憶在ＥＥＰＲＯＭ５０之許可鍵作爲鍵，而如下述地解碼

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

五、發明說明（８）

，生成解碼鍵ｓｋ´。

sk'=Dec(license_key,e)

然而，此處，Ｄｅｃ（Ａ，Ｂ）係爲意味著以共通鍵密碼方式用鍵Ａ，而解碼資料Ｂ。

然而，以此共通鍵密碼化方式之密碼化運算，已知有ＤＥＳ。針對共通鍵密碼化方式也是在上述過之 Applied Cryptography（Second Edition）已被詳細解過。

在於ＤＶＤ播放器１，在步驟Ｓ５所生成之鍵ｌｋ形成爲與被記憶在個人電腦２的ＥＥＰＲＯＭ５０（license_key）同一之值。即是成立下式。

lk=license_key

因此，在於各個電腦２，在步驟Ｓ１０所解碼而得到之鍵ｓｋ´，係爲在於ＤＶＤ播放器７，形成爲與在步驟Ｓ６所生成之密碼鍵ｓｋ同一之值。即是成立下式。

ｓｋ´＝ｓｋ

此樣，在於ＤＶＤ播放器１（始源端）及個人電腦２（接收端）的兩者，可以共有同一的鍵ｓｋ，ｓｋ´。在該處，將此鍵ｓｋ原樣作爲密碼鍵所用，或是以此爲根基

五、發明說明（９）

，分別作成疑似亂數，將此用作爲密碼鍵。

許可鍵，係爲由於是在各裝置根據對應於固有的ＩＤ及所提供的資訊之服務鍵而被生成，所以其他裝置無法生成ｓｋ或是ｓｋ´。另外，著作權者所未認可之裝置，因未具有許可鍵，所以無法生成ｓｋ或ｓｋ´。因此，其後ＤＶＤ播放器１使用密碼鍵ｓｋ，將再生資料密碼化後傳輸到個人電腦２時，當個人電腦２得到適切的許可鍵之情況，因具有密碼鍵ｓｋ´，所以可以解碼由ＤＶＤ播放器所傳輸到來的被密碼化再生資料。不過，個人電腦２未得到適切的許可鍵時，因未具有暗碼鍵ｓｋ´，所以無法解碼傳輸到來所被密碼化之再生資料。換言之，因只有適切的裝置可以生成共通的暗碼鍵ｓｋ，ｓｋ´，結果是形成爲進行鑑認。

如果１台個人電腦２的許可鍵被盜用，因ＩＤ爲每台相異，所以用該許可鍵，其他裝置無法解碼從ＤＶＤ播放器１傳輸到來所被密碼化之資料。因此，提高安全性。

第６圖係爲表示對於始源端（ＤＶＤ播放器１），不只是個人電腦２，磁光碟裝置３也是作爲接收端功能時之處理例。

此情況，在作爲接收端１的個人電腦２之ＥＥＰＲＯＭ５０，記憶有ＩＤ１作爲ＩＤ，另外記憶有license_key１作爲許可鍵；在於作爲接收端２之磁光碟裝置３，也是在ＥＥＰＲＯＭ３７，記憶有ＩＤ２作爲ＩＤ，另外記憶有license_key２作爲許可鍵。

五、發明說明（10）

在於ＤＶＤ播放器１（始源）與個人電腦２（接收１）之間所進行之步驟Ｓ１１至步驟Ｓ２０的處理，由於是與第４圖的步驟Ｓ１至步驟Ｓ１０的處理實質上爲同樣的處理，所以其說明省略。

即是，如上述，ＤＶＤ播放器１，對於個人電腦２進行鑑認處理。然後，在於步驟Ｓ２１，ＤＶＤ播放器１，對於磁光碟裝置３，要求ＩＤ。在於磁光碟裝置３，在步驟Ｓ２２介由１３９４介面３６，收訊此ＩＤ要求訊號，則該固件３０（第１０圖），在步驟Ｓ２３讀出被記憶在ＥＥＰＲＯＭ３７之ＩＤ（ＩＤ２），將此ＩＤ從１３９４介面３６，介由１３９４匯流排１１而被傳輸到ＤＶＤ播放器１。ＤＶＤ播放器１的固件２０，在步驟Ｓ２４，介由１３９４介面２６，而接受此ＩＤ２，則在步驟Ｓ２５，從下式生成鍵ｌｋ２。

lk2=hash(ID | | serviec_key)

進而，固件２０，在步驟Ｓ２６運算下式，將在步驟Ｓ１６所生成之鍵ｓｋ，使用在步驟Ｓ２６所生成之鍵ｌｋ２而密碼化，生成已密碼化的資料ｅ２。

然後，在步驟Ｓ２７，固件２０，將此密碼化資料ｅ２，從１３９４介面２６介由１３９４匯流排１１而傳輸到磁光碟裝置３。

在於磁光碟裝置３，在步驟Ｓ２８，介由１３９４介

五、發明說明（11）

面３６，收訊此密碼化資料ｅ２，在步驟Ｓ２９，運算下式，而生成密碼鍵ｓｋ２´。

sk2'=Dec(license_key2,e2)

如上述，在於個人電腦２及磁光碟裝置３分別得到密碼鍵ｓｋ１´，ｓｋ２´。這些之值形成爲與在ＤＶＤ播放器１之密碼鍵ｓｋ同一之值。

在於第６圖的處理例，ＤＶＤ播放器１，對於個人電腦２及磁光碟裝置３，分別要求個別的ＩＤ，使其處理，但能以通報通訊要求ＩＤ時，能進行如第７圖所示的處理。

即是，在於第７圖的處理例，在步驟Ｓ４１，作爲始源端之ＤＶＤ播放器１，對於全部的接收端（此例的情況，個人電腦２及磁光碟裝置３）以通報通訊要求ＩＤ。個人電腦２及磁光碟裝置３，分別在步驟Ｓ４２及步驟Ｓ４３，接受此ＩＤ傳送要求的訊號，則分別在步驟Ｓ４４及步驟Ｓ４５，讀出被記憶在ＥＥＰＲＯＭ５０或是ＥＥＰＲＯＭ３７之ＩＤ１或是ＩＤ２，將此ＩＤ１或是ＩＤ２傳輸到ＤＶＤ播放器１。ＤＶＤ播放器１，在步驟Ｓ４６及步驟Ｓ４７，分別收訊這些ＩＤ。

在於ＤＶＤ播放器，進而在步驟Ｓ４８，由下式生成密碼鍵ｌｌｋ１。

（請先閱讀背面之注意事項再填寫本頁）

訂

五、發明說明（12）

lk1=hash(ID1 | | serviec_key)

進而，在於步驟Ｓ４９，由下式生成密碼鍵ｌｋ２。

lk2=hash(ID2 | | serviec_key)

在於ＤＶＤ播放器１，進而在步驟Ｓ５０，生成密碼鍵ｓｋ，在步驟Ｓ５１，如下式所示，密碼鍵ｓｋ，將鍵ｌｋ１作爲鍵而被密碼化。

e1=Enc(lk1,sk)

進而，在於步驟Ｓ５２，密碼鍵ｓｋ，將鍵ｌｋ２作爲鍵，根據次式而被密碼化。

e2=Enc(lk2,sk)

進而，在於步驟Ｓ５３，ＩＤ１，ｅ１，ＩＤ２，ｅ２，分別如下式所示而被結合，生成密碼化資料ｅ。

e=ID1 | | e1 | | ID2 | | e2

在於ＤＶＤ播放器１，進而在步驟Ｓ５４，經上述過程所生成之密碼化資料ｅ，以通報通訊被傳輸到個人電腦

五、發明說明（13）

2及磁光碟裝置3。

在於個人電腦2及磁光碟裝置3，分別在步驟S55或是步驟S56，收訊這些密碼化資料e。然後，在於個人電腦2及磁光碟裝置3，分別在步驟S57或是步驟S58，進行下式所示之運算，生成密碼鍵sk1'，sk2'。

sk1'=Dec(license_key1,e1)

sk2'=Dec(license_key2,e2)

第8圖係爲表示使其1個的接收端能接受複數個服務（解碼複數個種類之資訊）的情況之處理例。即是，在於此情況，例如作爲接收端之個人電腦2，將複數個許可鍵（license_key1, license_key2, license_key3等）記憶在EEPROM。作爲始源端之DVD播放器1，在該EEPROM27記憶複數個服務鍵（service_key1, service_key2, service_key3等）。此情況，DVD播放器1，在步驟S81對於作爲接收端之個人電腦2要求ID時，DVD播放器1，傳送識別從此處所傳送的資訊（服務）之service_ID。在於個人電腦2，在步驟S82，收訊此service_ID時，從被記憶在EEPROM50之複數個許可鍵當中，選擇對應於此service_ID之資訊，用此資訊，在步驟S90進行解碼處理。其他的動作，與第4圖的情況同樣。

五、發明說明（14）

第９圖係爲表示另外的處理例。在於此例，作爲始源端的ＤＶＤ播放器１，在其ＥＥＰＲＯＭ２７，記憶service_key，ｈａｓｈ函數，及疑似亂數產生函數ｐＲＮＧ。這些則是著作權者所提供，且被秘密的保管。另外，在作爲接收端之個人電腦２之ＥＥＰＲＯＭ５０，具有從著作權者所供予的ＩＤ，ＬＫ，ＬＫ´，函數Ｇ，及疑似亂數產生函數ｐＲＮＧ。

ＬＫ係爲著作權者所作成之特異性亂數；ＬＫ´係爲使其滿足而被生成。

LK'=G^-1(R)

R=pRNG(H)(+)pRNG(LK)

H=hash(ID | | service-key)

然而，Ｇ^－１係爲意味著Ｇ的反函數。Ｇ^－１具有若爲已知所定的規則，則能簡單地計算，但若爲未知時，則不易計算之特徵。作爲此樣的函數，可以利用被用於公開密碼鍵之函數。

另外，疑似亂數產生函數，也能使其作爲軟體而設置。

ＤＶＤ播放器１的固件２０，最初在於步驟Ｓ１０１，對於個人電腦２的許可管理６２要求ＩＤ。個人電腦２的許可管理６２，在步驟Ｓ１０２，接受ＩＤ要求訊號，則讀出被記憶在ＥＥＰＲＯＭ５０的ＩＤ，在步驟

五、發明說明（15）

Ｓ１０３，將此ＩＤ傳輸到ＤＶＤ播放器１。ＤＶＤ播放器１的固件２０，在步驟Ｓ１０４接受此ＩＤ，則在步驟Ｓ１０５，運算下式

H=hash(ID | | service_key)

進而，固件２０，在步驟ｓ１０６，生成鍵ｓｋ，在步驟Ｓ１０７，運算下式

e=sk(+)pRng(H)

然而，Ａ（＋）Ｂ係爲意味著運算Ａ與Ｂ的排他邏輯和。

即是在疑似亂數產生鍵ｐＲＮＧ輸入在步驟Ｓ１０５所求得的Ｈ而得到之結果，運算ｐＲＮＧ（Ｈ）及在步驟Ｓ１０６所生成之鍵ｓｋ的每位元之排他邏輯和，而將鍵ｓｋ暗碼化。

其次，在步驟Ｓ１０８，固件２０將ｅ傳輸到個人電腦。

在於個人電腦２，在步驟Ｓ１０９收訊此ｅ，且在步驟Ｓ１１０，運算下式。

sk'=e(+)G(LK')(+)pRNG(LK)

五、發明說明（16）

即是運算在從ＤＶＤ播放器１所傳輸到來的ｅ，被記憶在ＥＥＰＲＯＭ５０的函數Ｇ，仍然適用被記憶在ＥＥＰＲＯＭ５０的ＬＫ´而得到之值Ｇ（ＬＫ´），並且將被記憶在ＥＥＰＲＯＭ５０之ＬＫ´，仍然適用於被記憶在ＥＥＰＲＯＭ５０之疑似亂數產生函數而得到的結果ｐＲＮＧ（ＬＫ）之排他邏輯和。

此處，如下式所示，形成爲ｓｋ＝ｓｋ´

$$
\begin{aligned}
sk' &= e(+)G(LK')(+)pRNG(LK) \\
&= sk(+)pRNG(H)(+)R(+)pRNG(LK) \\
&= sk(+)pRNG(H)(+)pRNG(H)(+)pRNG(LK)(+)pRNG(LK) \\
&= sk
\end{aligned}
$$

經此樣，作爲始源端之ＤＶＤ播放器１及作爲接收端之個人電腦２，可以共有同一的鍵ｓｋ，ｓｋ´。因可以作成ＬＫ，ＬＫ´只有著作權者，所以接收端爲不正常，就是欲作成ＬＫ，ＬＫ´也不能製作，可以更提高安全性。

在於上述，已經使其在於始源端與接收端進行鑑認，但例如在個人電腦２，通常可以載入任意的應用程式後使用。然且，作爲此應用程式，也有使用不當作成之情況。因此，在各應用程式，必須判定否從著作權者得到許可。此處，如第３圖所示，在於各應用部６１與許可管理６２之間，也如上述過，可以使其進行鑑認處理。此情況，許

（請先閱讀背面之注意事項再填寫本頁）

訂

經濟部中央標準局員工消費合作社印製

五、發明說明（17）

可管理６２形成爲始源端，應用部６１形成爲接收端。

其次，如上述，說明進行鑑認後（進行共有密碼鍵後），用密碼鍵，將從始源端所密碼化之資料傳輸到接收端，在於接收端，解碼此所密碼化的資料時的動作。

如第１０圖所示，如ＤＶＤ播放器１，或是磁光碟裝置３，在於內部的功能未開放給一般使用者之裝置，介由１３９４匯流排１１而收授的資料之密碼化及解碼的處理，分別以１３９４介面２６或是１３９４介面３６而進行。在此密碼化及解碼化，使用時段鍵Ｓ及時變鍵ｉ，但此時段鍵Ｓ及時變鍵ｉ（正確的是爲了生成時變鍵ｉ之鍵ｉ´），分別從固件２０或是固件３０，供給到１３９４介面２６或是１３９４介面３６。時段鍵Ｓ係爲以作爲初期值所用之初期值鍵Ｓｓ及爲攪亂時變鍵ｉ所用之攪亂鍵Ｓｉ而被構成。此初期值鍵Ｓｓ及攪亂鍵Ｓｉ，可以使其以在於上述過的鑑認所生成之暗碼鍵ｓｋ（＝ｓｋ´）的所定位元數之上位位元及下位位元，而分別構成。此時段鍵Ｓ，在每個時段（例如，每１個的電影資訊，或是每１次的再生），適當地被更新。對於此點，攪亂鍵Ｓｉ及從鍵ｉ所生成之時變鍵ｉ，係爲在於１個的時段內，頻繁地被更新之鍵；例如，可以使用在所定時間之時刻資訊等。

現今，將從作爲始源端之ＤＶＤ播放器１所再生輸出的影像資料，介由１３９４匯流排１１而傳輸到磁光碟裝置３及個人電腦２，針對各個解碼。此情況，針對ＤＶＤ播放器１，在於１３９４介面２６，用時段鍵Ｓ及時變鍵

五、發明說明（18）

i，進行密碼化處理。針對磁光碟裝置3，在於1394介面36，用時段鍵S及時變鍵i，進行解碼處理。

對於此點，在於個人電腦2，許可管理62，時段鍵S當中，將初期值鍵Ss供給到應用部61，且將攪亂鍵Si及時變鍵i（正確的是爲了生成時變鍵i之鍵i´）供給到1394介面49（連結部分）。然後，在於1394介面49，從攪亂鍵Si及鍵i´生成時變鍵i，用時變鍵i進行解碼，將該所被解碼的資料，在於應用部61，進而用時段鍵S（正確的是初期值鍵Ss），進行解碼。

此樣，在於個人電腦2，內部匯流排51，因被開放給使用者，所以以1394介面49只進行第1階段的解碼，仍是密碼的狀態。然後，在於應用部61，進而進行第2階段的解碼，成爲語體文。由於此因，對於個人電腦2，適切地附加功能，而使其禁止將在於內部匯流排51所收授的資料（語體文）複製到硬碟47或其他裝置。

此樣，在於本發明的實施形態，針對內部匯流排未被開放的CE裝置，用時段鍵S及時變鍵，進行1次密碼化或是解碼處理，但針對內部匯流排已被開放之裝置（個人電腦2等），區分成用時變鍵i之解碼處理，及用時段鍵S之解碼處理而進行解碼處理。此樣，使其可以具有1階段的解碼處理，及分成2階段解碼處理之兩者，必須使其成立下式。

（請先閱讀背面之注意事項再填寫本頁）

訂

線

五、發明說明（19）

Dec(S,Dec(I,Enc(algo(S+I),Data))=Data

然而，在於上述式，algo（S+i）係爲表示在所定的運算輸入時段鍵S及時變鍵i而得到的結果。

第11圖係爲表示滿足上述式之1394介面26的構成例。在於此構成例，以加法產生器71所生成之m位元的資料，被供給到收縮產生器73。另外，LFSR（Linear Feedback Shift Register）2輸出1位元的資料，供給到收縮產生器73。收縮產生器73，係爲對應於LFSR72的輸出，而選擇加法產生器71的輸出，將所選擇的資料作爲密碼鍵而輸出到加算器74。加算器74係爲加算所輸入的語體文（傳輸到1394匯流排11之m位元的資料），及由收縮產生器73所供給的m位元的資料（密碼鍵），將所加算的結果作爲語體文（所被密碼化的資料），而輸出到1394匯流排11。

加算器74的加算處理，係爲意味著以mod2^m（^爲冪次），加算收縮產生器73的輸出及語體文。換言之，加算m位元的同類資料，輸出忽視轉入之加算值。

第12圖係爲表示第11圖所示的1394介面26之更詳細構成例。從固件20所輸出的時段鍵S當中，初期值鍵Ss，介由加算器81而被傳輸到暫存器82且被保持。此初期值鍵Ss，例如以55字元（1字元具有8位元至32位元的寬度）而被構成。另外，從固件20所供給的時段S當中的例如以LSB側的32位元而被構成

（請先閱讀背面之注意事項再填寫本頁）

訂

線

五、發明說明（20）

之攪亂鍵Ｓｉ，被保持在暫存器８５。

在暫存器８４被保持有鍵ｉ´。此鍵ｉ´，例如介由１３９４匯流排１１而每次傳送１個組套，２位元的鍵ｉ´被供給到暫存器８４，１６組套分的（３２位元分的）鍵ｉ´被保持在暫存器８４時，以加算器８６，而與被保持在暫存器８５之３２位元的攪亂鍵Ｓｉ加算，作爲最終的時變鍵ｉ而被供給到加算器８１。加算器８１，係爲加算當時被保持在暫存器８２之值及由加算器８６所供給的時變鍵ｉ，將其加算結果供給到暫存器８２且使其保持。

暫存器８２的字元之位元數，例如爲８位元時，因由加算器８６所輸出的時變鍵ｉ爲３２位元，所以４分割時變鍵ｉ後使其將各８位元加算到暫存器８２的所定位址（０～５４）之文字。

經此樣，在暫存器８２，最初被保持有初期值鍵Ｓｓ，但其後，此值係爲在每次傳輸１６組套分的密碼文，以時變鍵ｉ而被更新。

加算器８３，係爲選擇被保持在暫存器８２之５５位元當中的所定２文字（第１２圖所示之時間的情況爲位址２３及位址５４的字元），加算該所選擇的２位元後，輸出至收縮產生器７３。另外，此加算器８３的輸出，在第１２圖所示的時間，則是被傳輸到暫存器８２的位址０，取代之前的保持值而被保持。

然後，在於次個時間，被供給到加算器８３之暫存器

（請先閱讀背面之注意事項再填寫本頁）

訂

線

經濟部中央標準局員工消費合作社印製

五、發明說明（21）

８２的２位元之位址，從位址５４及位址２３，只１位元分，朝圖中上方分別移動至位址５３及位址２２，以加算器８３的輸出而被更新的位址，也是圖中移動至更上方的位址。不過，比位址０還上方的位址因未存在，所以此情況，移動至位址５４。

然而，在加算器８１，８３，８６也能使其運算排他邏輯和。

ＬＦＳＲ７２，例如如第１３圖所示，以加算ｎ位元的移位暫存器１０１及移位暫存器１０１的ｎ位元當中的所定位元（暫存器）之值的加算器１０２而被構成。移位暫存器１０１，將由加算器１０２所供給的位元，保持在圖中最左側的暫存器b_n，則將至此被保持在該處的資料移位到右側的暫存器b_{n-1}。暫存器b_{n-1}，b_{n-2}，……也進行同樣的處理。然後，進而在次個時間，將以加算器１０２加算各位元之值所得之值，再度使其保持在圖中最左側的位元b_n。依順返復以上的動作，從圖中最右側的暫存器b_1依順輸出每１位元。

第１３圖係爲一般的構成例，但例如，更具體地，可以如第１４圖所示構成ＬＦＳＲ７２。在於此構成例，以３１位元構成移位暫存器１０１，以加算器１０２加算該圖中右端的暫存器b_1之值及左端的暫存器b_{31}之值，所被加算的結果使其回歸到暫存器b_{31}。

由ＬＦＳＲ７２所輸出的１位元資料爲邏輯１時，條件判定部９１，將由加法產生器７１的加算器８３所供給

（請先閱讀背面之注意事項再填寫本頁）

訂

線

經濟部中央標準局員工消費合作社印製

五、發明說明（22）

之m位元的資料原樣傳輸到ＦＩＦＯ９２且使其保持。對於此點，由ＬＦＳＲ７２所供給的１位元之資料爲邏輯０時，條件判定部９１，未接受由加算器８３所供給的m位元之資料，使其中斷密碼化處理。經此樣，在收縮產生器７３的ＦＩＦＯ９２，只選擇以加法產生器７１所生成之m位元的資料當中，ＬＦＳＲ７２輸出邏輯１的時間之資料且被保持。

以ＦＩＦＯ９２所保持的m位元之資料，作爲密碼鍵，而被供給到加算器７４，加算到應被傳輸的語體文之資料（從ＤＶＤ的再生資料），生成密碼文。

所被密碼化之資料，從ＤＶＤ播放器１介由１３９４匯流排１１而被供給到磁光碟裝置３及個人電腦２。

磁光碟裝置３，在於１３９４介面，爲了解碼從１３９４匯流排１１所收訊的資料，而具有如第１５圖所示之構成。在於此構成例，加法產生器１７１所輸出的m位元之資料，及ＬＦＳＲ所輸出的１位元之資料被供給到收縮產生器１７３。然後，收縮產生器１７３所輸出的m位元之鍵，被供給到減算器１７４。減算器１７４，從密碼文減算由收縮產生器１７３所供給之鍵，而解碼語體文。

即是第１５圖所示之構成係爲與第１１圖所示的構成基本上爲同樣的構成；在第１１圖的加算器７４，只有變更成減算器１７４之點爲相異。

第１６圖係爲表示第１５圖所示的構成之更詳細成例

（請先閱讀背面之注意事項再填寫本頁）

訂

線

五、發明說明（23）

。此構成基本上也是與第１２圖所示的構成同樣的構成，但在第１２圖之加算器７４被變更成減算器１７４。其他的加法產生器１７１，ＬＦＳＲ１７２，收縮產生器１７３，加算器１８１，暫存器１８２，加算器１８３，暫存器１８４，１８５，加算器１８６，條件判定部１９１，ＦＩＦＯ１９２等係爲對應於在第１２圖的加法產生器７１，ＬＦＳＲ７２，收縮產生器７３，加算器８１，暫存器８２，加算器８３，暫存器８４，８５，加算器８６，條件判定部９１，及ＦＩＦＯ９２。

因此，其動作基本上是與第１２圖所示的情況相同，所以其說明省略，但在於第１６圖，由收縮產生器１７３的ＦＩＦＯ１９２所輸出之ｍ位元之鍵，在於減算器１７４，從暗碼文減算後而解碼語體文。

如上述，在於１３９４介面３６，用時段鍵Ｓ（初期値鍵Ｓｓ及攪亂鍵Ｓｉ）及時變鍵ｉ，而解碼１次密碼化資料。

對於此點，如上述，在於個人電腦２，針對１３９４介面４９及應用部６１，分別分成２階段而進行解碼。

第１７圖係爲表示在於１３９４介面４９，進行解碼的情況之構成例。其基本構成係爲與第１５圖所示的情況同樣。即是在於此情況也是以加法產生器２７１，ＬＦＳＲ２７２，收縮產生器２７３及減算器２７４，構成１３９４介面４９；這些係爲與在第１５圖的加法產生器１７１，ＬＦＳＲ１７２，收縮產生器１７３，及減算

（請先閱讀背面之注意事項再填寫本頁）

訂

線

五、發明說明（24）

器，基本上是同樣的構成。不過，在於第１７圖的構成例，對於加法產生器２７１，作爲爲了從許可管理６２，生成時變鍵ｉ之鍵ｉ´，及時段鍵Ｓ當中，爲了攪亂時變鍵ｉ之攪亂鍵Ｓｉ，係爲供給與在第１５圖的情況同樣的鍵，但作爲初期值鍵Ｓｓ，係爲供給全部的位元爲０之單位元。

即是如第１８圖所示，因初期值鍵Ｓｓ的全部位元設爲０，所以實質上，與初期值鍵Ｓｓ爲存在的情況同樣地，根據時變鍵ｉ而生成密碼鍵。其結果，在於減算器２７４，根據密碼文的時變鍵ｉ只進行解碼。因尚未根據初期值鍵Ｓｓ進行解碼，所以此解碼結果所得的結果之資料，未形成爲完全的語體文，而是形成爲密碼文的狀態。因此，從內部匯流排５１載入此資料，記錄至硬碟４７，或其他記錄媒體，也無法原樣利用該資料。

然且，如上述，在於１３９４介面４９，硬體式的根據時變鍵ｉ而軟體式的解碼所被解碼的資料之應用部６１的構成，係爲如第１９圖所示，以加法產生器３７１，ＬＦＳＲ３７２，收縮產生器３７３及減算器３７４而被構成。其基本構成形成爲與第１５圖所示的加法產生器１７１，ＬＦＳＲ１７２，收縮產生器１７３及減算器１７４同樣的構成。

不過，時段鍵Ｓ當中，初期值鍵Ｓｓ，係爲與第１５圖的情況同樣地，供給一般的初期值鍵，但爲了生成時變鍵ｉ之攪亂鍵Ｓｉ及鍵ｉ，分別是全部的位元爲０之單位

（請先閱讀背面之注意事項再填寫本頁）

訂

線

五、發明說明（25）

元的資料。

其結果，在第２０圖表示其詳情（其加法產生器３７１及ＦＦＯ３９２，係爲對應於第１６圖的加法產生器１７１及Ｆ１ＦＯ１９２），被保持在暫存器３８４之鍵ｉ′及被保存在暫存器３８５之攪亂鍵Ｓｉ，由於全部的位元爲０，所以加算器３８６所輸出的時變鍵ｉ也是全部的位元形成爲０，實質上進行與時變鍵ｉ未存在的情況同樣的動作。即是只根據初期值鍵Ｓｓ生成密碼鍵。然後，在於減算器３７４，根據經此過程所生成之密碼鍵，密碼文被解碼成語體文。如上述，此密碼文，因在於１３９４介面４９，根據時變鍵ｉ而進行第１階段的解碼，所以在此處，根據初期值鍵Ｓｓ進行第２階段的解碼，而可以得到完全的語體文。

在於磁光碟裝置３，經上述過程而解碼密碼文，則ＣＰＵ３１，將所被解碼的資料供給到驅動器３５，且使其記錄至磁光碟。

另則，在於個人電腦２，ＣＰＵ４１（應用部６１），將經上述所被解碼的資料，例如供給到硬碟４７且使其記錄。在於個人電腦２，可以以擴充埠４８連接所定的連接埠，而監視在內部匯流排５１所收授的資料，但可以最終的解碼被傳輸到內部匯流排５１的資料，就是爲應用部６１，所以可以監視擴充埠４８，以１３９４介面，根據時變鍵ｉ進行解碼之資料（尚未根據時段鍵Ｓ進行解碼之資料，也無法監視完全的恢復成語體文之資料。因此，可

（請先閱讀背面之注意事項再填寫本頁）

訂

線

五、發明說明（26）

以防止不當的複製。

然而，時段鍵的共有，例如也能使用 Diffie-Hellman 法等而使其進行。

然而，另外例如在個人電腦２之１３９４介面４９或是應用部６１的處理能力較低，無法進行解碼處理時，若在於始源端側，使其以單位元構成時段鍵與時變鍵的其中１個，或是兩者；在於接收端側，也是以單位元使用這些鍵，則實施上未使用時段鍵及時變鍵，形成爲能收授資料。不過，若爲此樣，則恐會增高資料的不當複製之疑慮。

應用部６１其資料，若爲不正複製的資料時，恐會有不當複製所被解碼的資料，但如上述，若使其以許可管理６２鑑認應用部６１，則能防止不當複製。

作爲此情況的鑑認方法，可以利用共通鍵密碼方式或是公開鍵密碼方式之數字式署名。

以上的第１１圖，第１２圖，第１５圖及第２０圖所示之構成，係爲滿足準同形（homomorphism）的關係之構成。即是鍵 K_1，K_2 爲伽羅瓦（Galois）領域 G 的要素時，兩者的群運算結果，K_1，K_2 也形成爲伽羅瓦領域 G 的要素。然且，進而針對所定的函數 H，成立下式。

$$H(K_1 \cdot K_2)=H(K_1) \cdot H(K_2)$$

第２１圖係爲進而表示１３９４介面２６的其他構成例。在於此構成例，使其時段鍵 S 被供給到

（請先閱讀背面之注意事項再填寫本頁）

訂

線

五、發明說明（27）

ＬＦＳＲ５０１至５０３，且被初期設定。

ＬＦＳＲ５０１至５０３之幅寬的n_1至n_3，分別以２０位元程度，各別的幅寬n_1至n_3爲相互地成爲因素而被構成。因此，例如時段鍵Ｓ當中，例如上位n_1位元被初期設定在ＬＦＳＲ５０１，其次的上位n_2位元被初期設定在ＬＦＳＲ５０２，進而其次的上位n_3位元初期設定在ＬＦＲ５０３。

ＬＦＳＲ５０１至５０３，由計時功能５０６，例如輸入邏輯１的能啓動訊號時，只ｍ位元進行移位動作，輸出ｍ位元的資料。ｍ之值例如可以設爲８，１６，３２，４０。

ＬＦＳＲ５０１及ＬＦＳＲ５０２之輸出，被輸入到加算器５０４，且被加算。加算器５０４的加算値當中，載體成分，被供給到計時功能５０６；ｓｕｍ成分，被供給到加算器５０５，與ＬＦＳＲ５０３的輸出加算。加算器５０５的載體成分，被供給到計時功能５０６；ｓｕｍ成分，被供給到排他邏輯和電路５０８。

計時功能５０６，由於是由加算器５０４及加算器５０５所供給的資料組合爲００，０１，１０，１１的其中１個，所以對應於這些，而對ＬＦＳＲ５０１至５０３，輸出０００至１１１的其中１個之組合資料。

ＬＦＳＲ５０１至５０３，係爲在輸入邏輯１時，進行ｍ位元的移位動作，且輸出新的ｍ位元之資料；輸入邏輯０時，輸出與前次所輸出的情況同一ｍ位元之資料。

（請先閱讀背面之注意事項再填寫本頁）

訂

線

五、發明說明（28）

排他邏輯和電路５０８，係爲運算加算器５０５所輸出的ｓｕｍ成分及被保持在暫存器５０７的時變鍵ｉ之排他邏輯和，將其運算結果輸出至排他邏輯和電路５０９。排他邏輯和電路５０９，係爲運算所被輸入的語體文，及由排他邏輯和電路５０８所輸入之密碼鍵的排他邏輯和，將運算結果作爲密碼後輸出。

第２２圖係爲表示在磁光碟裝置３的１３９４介面３６之構成例。在此構成例之ＬＦＳＲ６０１至排他邏輯和電路６０９，係爲與第２１圖的ＬＦＳＲ５０１至排他邏輯和５０９同樣的構成。因此，該動作基本上也是同樣，所以省略其說明。不過，對於在於第２１圖的構成例，進行密碼化處理；在於第２２圖的構例，則是進行解碼處理。

第２３圖係爲表示個人電腦２的１３９４介面４９之構成例。在此構成例之ＬＦＳＲ７０１至排他邏輯和電路７０９，也是與在第２２圖的ＬＦＳＲ６０１至排他邏輯和電路６０９同樣的構成。不過，被初期設定在ＬＦＳＲ７０１至７０３之時段鍵Ｓ，係爲全部的位元爲０單位元。因此，此情況，實質上只對應於被保持在暫存器７０７之時變鍵ｉ而進行解碼化處理。

第２４圖係爲表示個人電腦２的應用部６１之構成例。在此構成例之ＬＦＳＲ８０１至排他邏輯和電路８０９，係爲與在第２圖之ＬＦＳＲ６０１至排他邏輯和電路６０９基本上是同樣的構成。不過，被輸入至暫存器

（請先閱讀背面之注意事項再填寫本頁）

訂

線

五、發明說明（29）

807之時變鍵i，只有全部的位元爲0單位之點爲相異。因此，此構成例的情況，只根據時段鍵S而生成密碼鍵，進行解碼處理。

然而，第19圖，第20圖及第24圖所示之處理，由於是在於應用部61而進行，因而是軟性式的處理。

在於上述，將DVD播放器作爲始源端，將個人電腦2及磁光碟裝置3作爲接收端，但將任何的裝置作爲始源端或是接收端爲任意。

另外，連接各電子機器之外部匯流排，也不限於1394匯流排，可以利用種種的匯流排，連接至該匯流排之電子機器，也是不限於上述過之例，任意的裝置皆可。

〔發明效果〕

如上述，依據申請專利第1項及申請專利第9項之密碼化方法，由於用第1鍵，及將資料密碼化時，在所定時間所被變更的第2鍵而使其生成暗碼鍵，所以能更安全地進行密碼化。

依據申請專利第10項及申請專利第13項，由於用第1鍵，及解碼資料時，在所定時間所被變更的第2鍵而使其生成密碼鍵，所以能更安全地解碼所被密碼化的資料。

依據申請專利第14項之資訊處理系統及申請專利第15項之資訊處理方法，在於功能變更未開放給使用者之

五、發明說明（30）

第１資訊處理裝置，用第１鍵，及解碼資料時，在所定時間所被變更的第２鍵，而使其生成密碼鍵；在於功能變更被開放給使用者之第２資訊處理裝置，用第１鍵及第２鍵的一方，生成之第１密碼鍵，解碼所被密碼化的資料，用第１鍵及第２鍵的他方所生成之第２密碼鍵，進而使其解碼該所被解碼的資料，所以能實現更安全的資訊處理系統。

依據申請專利第１６項之資訊處理裝置及申請專利第１７項之資訊處理方法，由於以軟體程式使其生成第１鍵，及解碼資料時，在所定時間所被變更的第２密碼鍵，所以能在每個應用程式進行解碼，且能更確實地防止不當的複製。

〔圖面之簡單說明〕

第１圖係爲表示適用本發明的資訊處理系統構成例之方塊圖。

第２圖係爲表示第１圖的ＤＶＤ播放器１，個人電腦２，及磁光碟裝置的內部構成例之方塊圖。

第３圖係爲說明鑑認處理之圖。

第４圖係爲說明鑑認處理之時間圖。

第５圖係爲表示node_unique_ID的格式之圖。

第６圖係爲說明其他的鑑認處理之時間圖。

第７圖係爲說明另外的鑑認處理之時間圖。

第８圖係爲說明其他的鑑認處理之時間圖。

五、發明說明（31）

第９圖係爲說明其他的鑑認處理之時間圖。

第１０圖係爲說明密碼化處理之方塊圖。

第１１圖係爲表示第１０圖１３９４介面２６的構成例之方塊圖。

第１２圖係爲表示第１１圖１３９４介面２６的更詳細構成例之方塊圖。

第１３圖係爲表示第１２圖ＬＦＳＲ７２的更詳細構成例之方塊圖。

第１４圖係爲表示第１３圖ＬＦＳＲ７２的更具體構成例之方塊圖。

第１５圖係爲表示第１０圖１３９４介面３６的構成例之方塊圖。

第１６圖係爲表示第１５圖１３９４介面３６的更詳細構成例之方塊圖。

第１７圖係爲表示第１０圖１３９４介面４９的構成例之方塊圖。

第１８圖係爲表示第１７圖１３９４介面４９的更詳細構成例之方塊圖。

第１９圖係爲表示第１０圖應用部６１的構成例之方塊圖。

第２０圖係爲表示第１９圖應用部６１的更詳細構成例之方塊圖。

第２１圖係爲表示第１０圖１３９４介面２６的其他構成例之方塊圖。

（請先閱讀背面之注意事項再填寫本頁）

訂

線

經濟部中央標準局員工消費合作社印製

五、發明說明（32）

第２２圖係爲表示第１０圖１３９４介面３６的其他構成例之方塊圖。

第２３圖係爲表示第１０圖１３９４介面３６的其他構成例之方塊圖。

第２３圖係爲表示第１０圖應用部６１的其他構成例之方塊圖。

〔圖號說明〕

１：ＤＶＤ播放器

２：個人電腦

３：磁光碟裝置

１１：１３９４匯流排

２０：固件

２１：ＣＰＵ

２５：驅動器

２６：１３９４介面

２７：ＥＥＰＲＯＭ

３１：ＣＰＵ

３５：驅動器

３６：１３９４介面

３７：ＥＥＰＲＯＭ

４１：ＣＰＵ

４７：硬體

４８：擴充埠

五、發明說明（33）

49：1394介面

50：EEPROM

51：內部匯流排

61：應用部

62：許可管理

六、申請專利範圍

1．一種密碼化裝置，其特徵爲具備：

用密碼鍵將資料密碼化之密碼化手段，及

產生第1鍵之第1鍵產生手段，及

當資料密碼化時，產生在所定時間所被變更的第2鍵之第2鍵產生手段，及

用前述第1鍵及第2鍵，生成前述密碼鍵之生成手段。

2．如申請專利範圍第1項之密碼化裝置，其中前述生成手段係爲生成準同形的密碼鍵。

3．如申請專利範圍第1項之密碼化裝置，其中前述生成手段係爲個別使用構成前述密碼鍵的第1密碼鍵及第2密碼鍵，而依順解碼所被密碼化的資料，生成正確解碼結果所得到的密碼鍵。

4．如申請專利範圍第1項之密碼化裝置，其中前述生成手段，係爲在以前述第1鍵作爲初期值之值，加算第2鍵，而生成前述密碼鍵。

5．如申請專利範圍第4項之密碼化裝置，其中前述第1鍵係爲比前述第2鍵還多的位元數；前述生成手段，係爲將前述第2鍵加算到前述第1鍵的所定位置之位元，抽出加算結果的所定位置之位元，進而加算到所抽出的位元，而生成前述密碼鍵。

6．如申請專利範圍第5項之密碼化裝置，其中前述生成手段，係爲以進而加算到前述所抽出的位元而得到之結果，進而更新前述加算結果的所定位元。

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

六、申請專利範圍

7．如申請專利範圍第6項之密碼化裝置，其中前述生成手段，係爲從進而加算到前述所抽出的位元而得到的結果當中，在所定的時間選擇所定的位元，而生成前述密碼鍵。

8．如申請專利範圍第1項之密碼化裝置，其中具備將以前述密碼鍵所密碼化之資料，介由匯流排而傳輸到其他裝置之傳輸手段。

9．一種密碼化方法，其特徵爲具備：

用密碼鍵將資料密碼化之密碼化步驟，及

產生第1鍵之第1產生步驟，及

將資料密碼化時，產生在所定時間所被變更的第2鍵之第2產生步驟，及

用前述第1鍵及第2鍵，生成前述密碼鍵之生成步驟。

10．一種解碼裝置，其特徵爲具備：

收訊所被密碼化的資料之收訊手段，及

用密碼鍵，解碼前述所收訊的資料之解碼手段，及

產生第1鍵之第1鍵產生手段，及

解碼資料時，產生在所定時間所被變更的第2鍵之第2產生手段，及

用前述第1鍵及第2鍵，生成前述密碼鍵之生成手段。

11．如申請專利範圍第10項之解碼裝置，其中前述生成手段，具備：

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

線

六、申請專利範圍

用前述第１鍵及第２鍵的一方，生成第１密碼鍵之第１生成手段，及

用前述第１鍵及第２鍵的他方，生成第２密碼鍵之第２生成手段；

前述解碼手段，具備：

用前述第１密碼鍵，解碼前述所被密碼化的資料之第１解碼手段，及

用前述第２密碼鍵，進而解碼以前述第１解碼手段而被解碼的資料之第２解碼手段。

１２．如申請專利範圍第１１項之解碼裝置，其中前述第２解碼手段，係爲以處理所被解碼的資料之應用軟體而被構成。

１３．一種解碼方法，其特徵爲具備：

收訊所被密碼化的資料之收訊步驟，及

用密碼鍵解碼前述所收訊的資料之解碼步驟，及

產生第１鍵之第１產生步驟，及

當解碼資料時，產生在所定時間所被變更的第２鍵之第２產生步驟，及

用前述第１鍵及第２鍵，生成前述密碼鍵之生成步驟。

１４．一種資訊處理系統，係爲針對以介由匯流排，相互連接的複數個資訊處理裝置，而被構成之資訊處理系統；其特徵爲：

前述資訊處理裝置，係爲以功能變更未開放給使用者

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

經濟部中央標準局員工消費合作社印製

六、申請專利範圍

之第 1 資訊處理裝置，及功能變更開放給使用者之第 2 資訊處理裝置等而被構成；

前述第 1 資訊處理裝置，具備：

收訊所被密碼化的資料之第 1 收訊手段，及

用密碼鍵，解碼前述第 1 收訊手段所收訊的資料之第 1 解碼手段，及

產生第 1 鍵之第 1 產生手段，及

當解碼資料時，產生在所定時間所被變更的第 2 鍵之第 2 產生手段，及

用前述第 1 產生手段所產生的第 1 鍵及前述第 2 產生手段所產生的第 2 鍵，生成前述密碼鍵之第 1 生成手段；

前述第 2 資訊處理裝置，具備：

收訊所被密碼化的資料之第 2 收訊手段，及

產生第 1 鍵之第 3 產生手段，及

當解碼資料時，產生在所定時間所被變更的前述第 2 鍵之第 4 產生手段，及

用前述第 3 產生手段所產生的第 1 鍵及前述第 4 產生手段所產生的第 2 鍵其一方，生成第 1 密碼鍵之第 2 生成手段；及

用前述第 3 產生手段所產生的第 1 鍵及前述第 4 產生手段所產生的第 2 鍵其他方，生成第 2 密碼鍵之第 3 生成手段；及

用前述第 1 密碼鍵，解碼前述收訊手段所收訊的密碼化資料之第 2 解碼手段，及

六、申請專利範圍

用前述第2密碼鍵，進而解碼以前述第2解碼手段而被解碼的資料之第3解碼手段。

15.一種資訊處理方法，係爲針對以介由匯流排，相互連接的複數個資訊處理裝置之資訊處理系統的資訊處理方法；其特徵爲：

前述資訊處理裝置，係爲以功能變更未被開放給使用者之第1資訊處理裝置，及功能變更開放給使用者之第2資訊處理裝置等而被構成；

前述第1資訊處理裝置，具備：

收訊所被密碼化的資料之第1收訊步驟，及

用密碼鍵，解碼在前述第1收訊步驟所收訊的資料之第1解碼步驟，及

產生第1鍵之第1產生步驟，及

當解碼資料時，產生在所定時間所被變更的第2鍵之第2產生步驟，及

用在前述第1產生步驟所產生的第1鍵及在前述第2產生步驟所產生的第2鍵，生成前述密碼鍵之第1生成步驟；

前述第2資訊處理裝置，具備：

收訊所被密碼密化的資料之第2收訊步驟，及

產生第1鍵之第3產生步驟，及

當解碼資料時，產生在所定時間所被變更的前述第2鍵之第4產生步驟，及

用在前述第3產生步驟所產生的第1鍵及在前述第4

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

六、申請專利範圍

產生步驟所產生的第２鍵其一方，生成第１密碼鍵之第２生成步驟；及

用在前述第３產生步驟所產生的第１鍵及前述第４產生步驟所產生的第２鍵其他方，生成第２密碼鍵之第３生成步驟；及

用前述第１密碼鍵，解碼在前述第２收訊步驟所收訊的被密碼化的資料之第２解碼步驟，及

用前述第２密碼鍵，進而解碼在前述第２解碼步驟所被解碼的資料之第３解碼步驟。

１６．一種資訊處理裝置，其特徵爲具備：

收訊介由匯流排而傳輸到來的資料之收訊手段，及

從前述收訊手段所收訊的資料，生成第１密碼鍵及當解碼資料時，在所定時間所被變更的第２密碼鍵之軟體程式所形成之生成手段，及

用前述生成手段所生成的第１密碼鍵及第２密碼鍵其一方，解碼前述收訊手段所收訊的被密碼化資料之第１解碼手段，及

用前述生成手段所生成的第１密碼鍵及第２密碼鍵其他方，進而解碼以前述解碼手段所被解碼的資料後作處理之軟體程式所形成之第２解碼手段。

１７．一種資訊處理方法，其特徵爲具備：

收訊介由匯流排而傳輸到來的資料之收訊步驟，及

從在前述收訊步驟所收訊的資料，生成第１密碼鍵及當解碼資料時，在所定時間所被變更的第２密碼鍵之軟體

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

六、申請專利範圍

程式所形成之生成步驟，及

用在前述生成步驟所生成的第1密碼鍵及第2密碼鍵其一方，解碼在前述收訊步驟所收訊的被密碼化的資料之第1解碼步驟，及

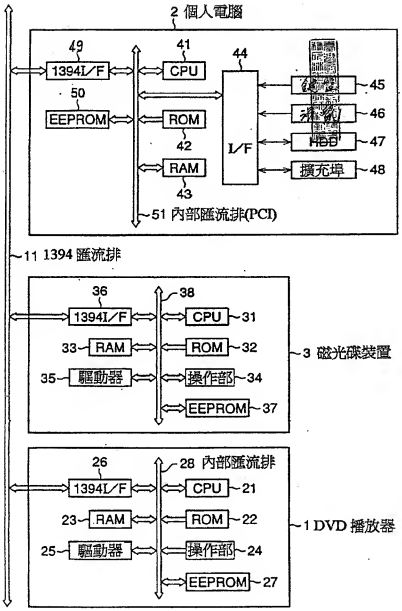
用在前述生成步驟所生成的第1密碼鍵及第2密碼鍵其他方，進而解碼在前述第1解碼步驟所被解碼的資料後作處理之軟體程式所形成之第2解碼步驟。

87105738

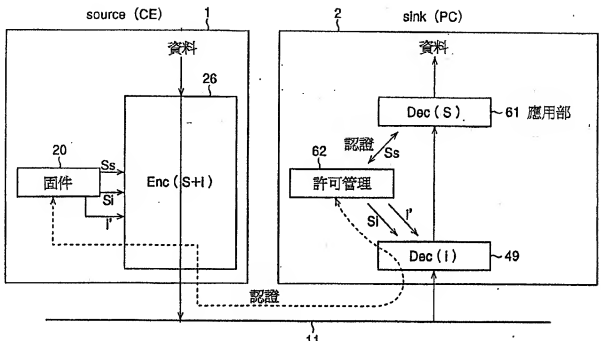
(1/ 23)

731163

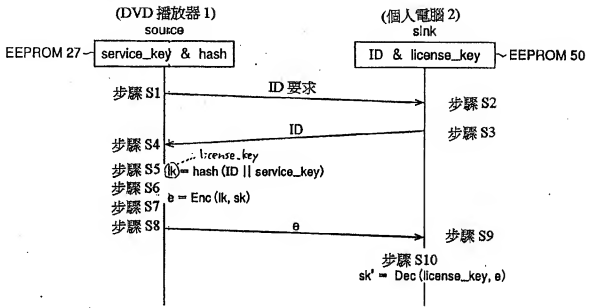
第 1 圖


2 個人電腦
49
1394I/F
41
CPU
44
50
EEPROM
ROM
42
RAM
43
I/F
45
46
HDD
47
擴充埠
48
51 內部匯流排(PCI)
11 1394 匯流排
36
1394I/F
38
CPU
31
33
RAM
ROM
32
35
驅動器
操作部
34
EEPROM
37
3 磁光碟裝置
26
1394I/F
28 內部匯流排
CPU
21
23
RAM
ROM
22
25
驅動器
操作部
24
EEPROM
27
1 DVD 播放器

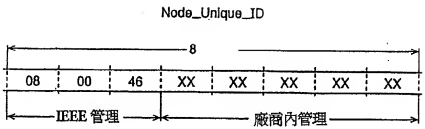
第 2 圖


source (CE)
1
2
sink (PC)
資料
資料
26
Dec (S)
61 應用部
20
Ss
固件
Enc (S-H)
62
認證
Ss
許可管理
Si
I'
Si
I'
Dec (I)
49
認證
11

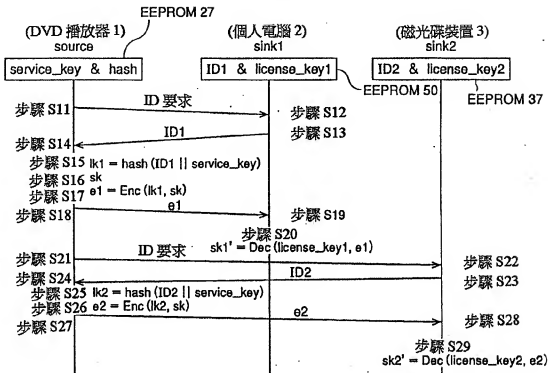
第 3 圖


(DVD 播放器 1)
source
(個人電腦 2)
sink
EEPROM 27
service_key & hash
ID & license_key
EEPROM 50
步驟 S1
ID 要求
步驟 S2
ID
步驟 S3
步驟 S4
license_key
步驟 S5
lk = hash (ID || service_key)
步驟 S6
步驟 S7
e = Enc (lk, sk)
步驟 S8
e
步驟 S9
步驟 S10
sk' = Dec (license_key, e)

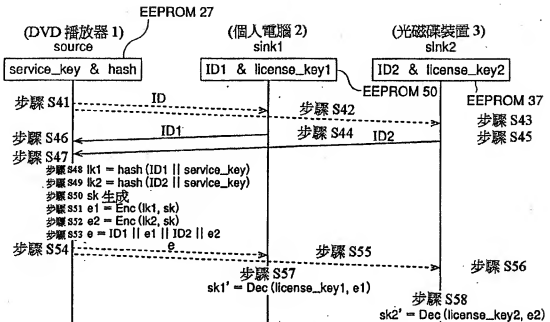
第 4 圖



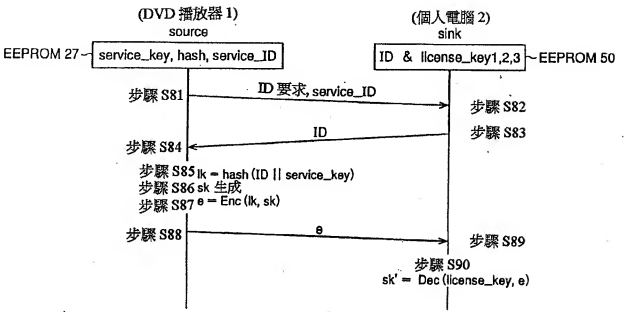
第 5 圖


EEPROM 27
(DVD 播放器 1)
source
(個人電腦 2)
sink1
(磁光碟裝置 3)
sink2
service_key & hash
ID1 & license_key1
ID2 & license_key2
EEPROM 50
EEPROM 37
步驟 S11
ID 要求
步驟 S12
步驟 S13
ID1
步驟 S14
步驟 S15 lk1 = hash (ID1 || service_key)
步驟 S16 sk
步驟 S17 e1 = Enc (lk1, sk)
步驟 S18
e1
步驟 S19
步驟 S20
sk1' = Dec (license_key1, e1)
步驟 S21
ID 要求
步驟 S22
步驟 S24
ID2
步驟 S23
步驟 S25 lk2 = hash (ID2 || service_key)
步驟 S26 e2 = Enc (lk2, sk)
步驟 S27
e2
步驟 S28
步驟 S29
sk2' = Dec (license_key2, e2)

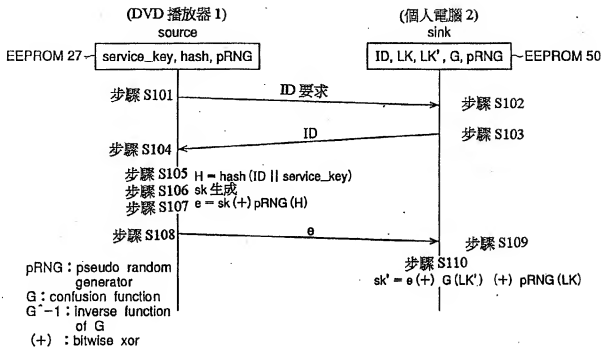
第 6 圖


EEPROM 27
(DVD 播放器 1)
source
(個人電腦 2)
sink1
(光磁碟裝置 3)
sink2
service_key & hash
ID1 & license_key1
ID2 & license_key2
EEPROM 50
EEPROM 37
步驟 S41
ID
步驟 S42
步驟 S43
步驟 S46
ID1
步驟 S44
ID2
步驟 S45
步驟 S47
步驟 S48 lk1 = hash (ID1 || service_key)
步驟 S49 lk2 = hash (ID2 || service_key)
步驟 S50 sk 生成
步驟 S51 e1 = Enc (lk1, sk)
步驟 S52 e2 = Enc (lk2, sk)
步驟 S53 e = ID1 || e1 || ID2 || e2
步驟 S54
e
步驟 S55
步驟 S56
步驟 S57
sk1' = Dec (license_key1, e1)
步驟 S58
sk2' = Dec (license_key2, e2)

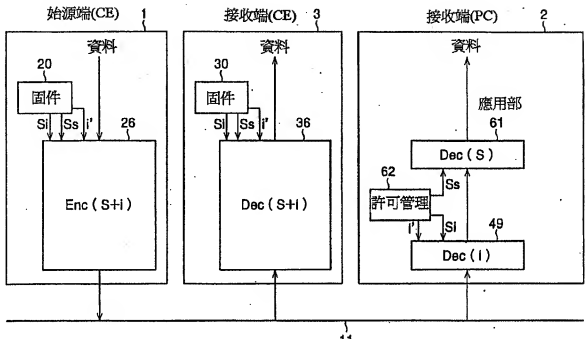
第 7 圖


(DVD 播放器 1)
source
EEPROM 27
service_key, hash, service_ID
(個人電腦 2)
sink
ID & license_key1,2,3
EEPROM 50
步驟 S81
ID 要求, service_ID
步驟 S82
步驟 S83
ID
步驟 S84
步驟 S85 lk = hash (ID || service_key)
步驟 S86 sk 生成
步驟 S87 e = Enc (lk, sk)
步驟 S88
e
步驟 S89
步驟 S90
sk' = Dec (license_key, e)

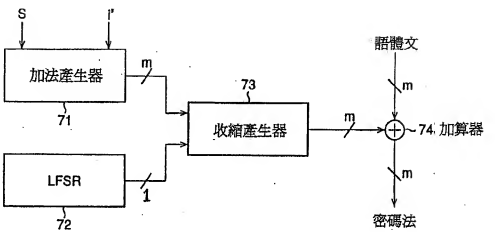
第 8 圖


(DVD 播放器 1)
source
EEPROM 27
service_key, hash, pRNG
(個人電腦 2)
sink
ID, LK, LK', G, pRNG
EEPROM 50
步驟 S101
ID 要求
步驟 S102
步驟 S103
ID
步驟 S104
步驟 S105 H = hash (ID || service_key)
步驟 S106 sk 生成
步驟 S107 e = sk (+) pRNG (H)
步驟 S108
e
步驟 S109
步驟 S110
sk' = e (+) G (LK') (+) pRNG (LK)
pRNG : pseudo random generator
G : confusion function
G^-1 : inverse function of G
(+) : bitwise xor

第 9 圖

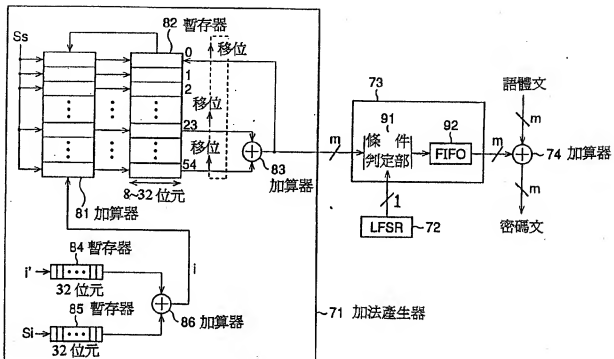

始源端(CE)
1
資料
20
固件
Si
Ss
i'
26
Enc (S+I)
接收端(CE)
3
資料
30
固件
Si
Ss
i'
36
Dec (S+I)
接收端(PC)
2
資料
應用部
61
Dec (S)
62
Ss
許可管理
i'
SI
49
Dec (I)
11

第10圖

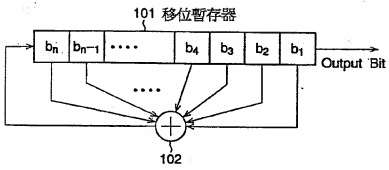


1394I/F 26
(始源端(CE))

第11圖

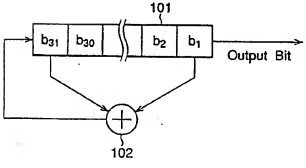

82 暫存器
Ss
0
移位
1
2
移位
23
移位
54
8~32 位元
81 加算器
83
加算器
m
73
91
條 件
判定部
92
FIFO
m
74 加算器
1
LFSR
72
語體文
m
m
密碼文
84 暫存器
i'
32 位元
i
85 暫存器
Si
32 位元
86 加算器
71 加法產生器
1394I/F 26
(接收端(CE))

第12圖



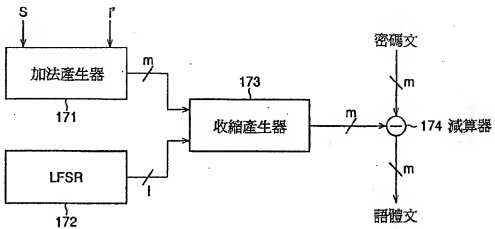
LFSR 72

第13圖



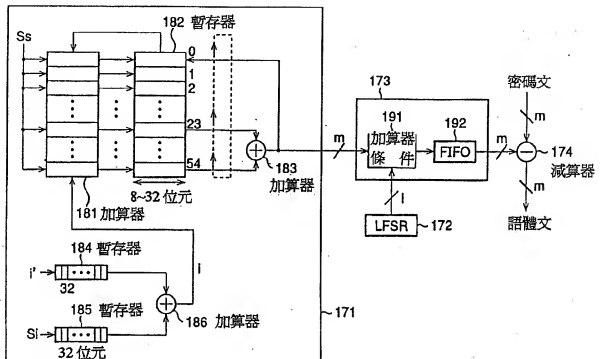
LFSR 72'

第14圖



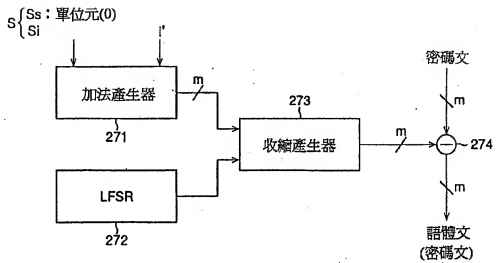
1394L/F 36
(接收端(CE))

第15圖



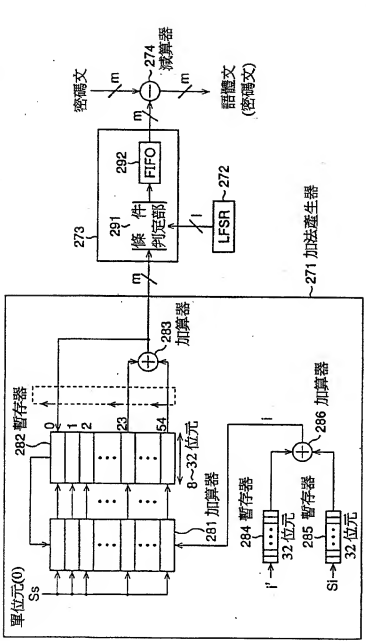
1394I/F 36
(接收端(CE))

第16圖



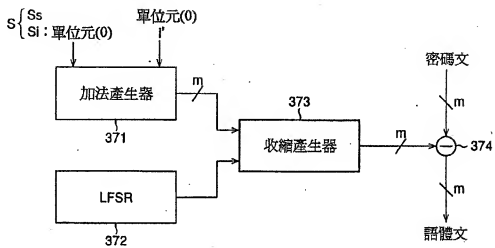
1394I/F49
(接收端(PC)的連結部分)

第17圖



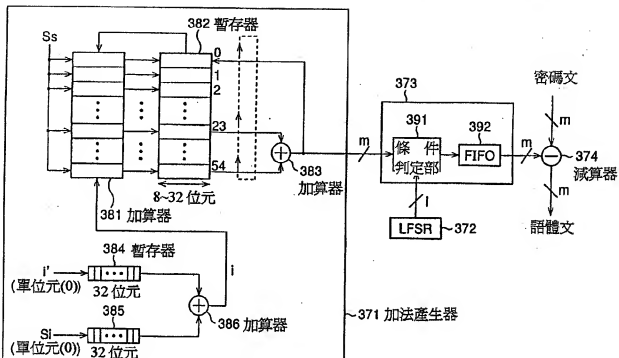
1394IJF49
(接收端(PC)的連結部分)

第 18 圖



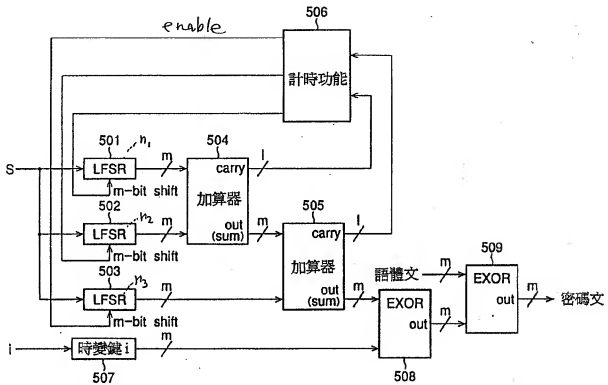
接收端(PC)的應用部 61

第 19 圖

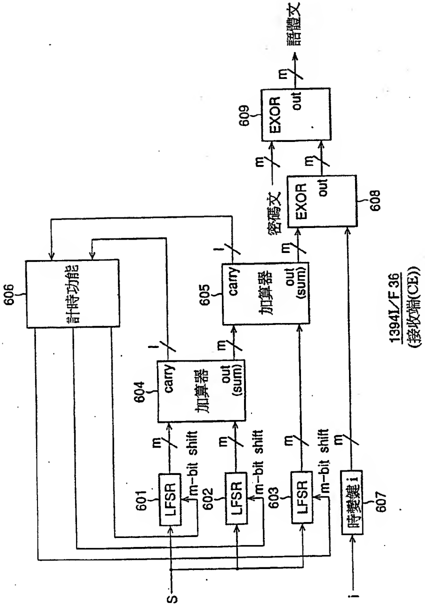


接收端(PC)的應用部 61

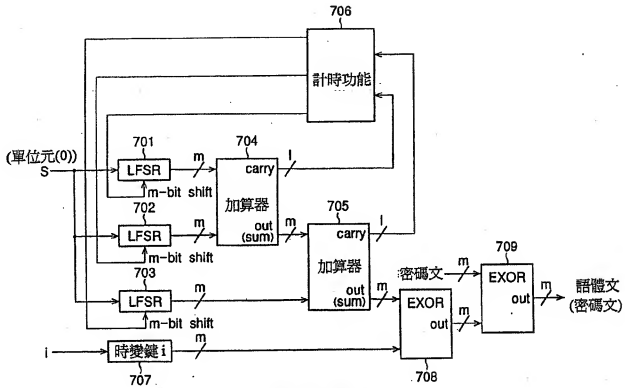
第20圖


enable
506
計時功能
501
n_1
LFSR
m
m-bit shift
S
504
carry
l
加算器
out
(sum)
502
n_2
LFSR
m
m-bit shift
505
carry
l
加算器
out
(sum)
503
n_3
LFSR
m
m-bit shift
語體文
m
509
EXOR
out
密碼文
EXOR
out
i
時變鍵 i
m
507
508
1394I/F 26
(始源端(CE))

第 21 圖


S
i
601
602
603
LFSR
LFSR
LFSR
m-bit shift
m-bit shift
m-bit shift
607
時變鍵 i
604
carry
加算器
out
(sum)
605
carry
加算器
out
(sum)
606
計時功能
l
l
m
密碼文
608
EXOR
out
609
EXOR
out
語體文
1394L/F36
(接收端(CE))

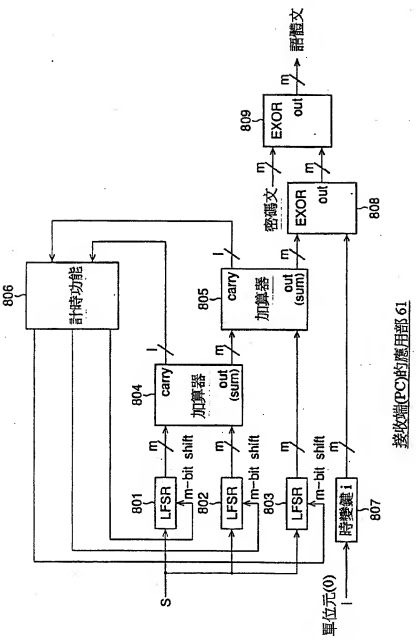
第22圖



1394I/F49

(接收端(PC)的連結部分)

第 23 圖



接收端(PC)的應用部 61

第 24 圖